Ohio Attorney General's

Consumer Advocate Newsletter

Keeping Consumers Safe and Informed

October 2023

How to respond to a data breach

Cybersecurity Awareness Month (October) serves as a reminder of the importance of preparing for potential data breaches and knowing how to respond when you learn that your personal information has been compromised.

What is a data or security breach?
A data or security breach is the unauthorized access to and acquisition of personal information which causes or reasonably is believed will cause a risk of identity theft.

What is "personal information"?
In Ohio, personal information is an individual's name connected with any of the following: Social Security number; Driver's license number or state identification card number; or account number, credit, or debit card number linked to a security code or password. Sometimes companies have a broader definition of personal information that may include a combination of username, password, email address, etc.

Do consumers need to be notified of a breach?
Under the Ohio Security Breach Notification Act, consumers must be notified of any security breach to stored personal information that may reasonably cause a material risk of identity theft or other fraud.

How quickly must a business notify consumers of a breach?
Consumers must be notified in the quickest way possible but not later than 45 days after the breach is discovered.

What is an acceptable notice of a breach?
The type of notice required depends on the number of consumers affected and the size of the business. Depending on these factors, it may be acceptable to notify consumers in writing; via e- mail or electronic notice; over the phone; through the local newspaper; on the business's website; or through notification to major media outlets in the area where the entity is located.

Here are some ways to protect yourself if you fall victim to a data breach:

- Read all notifications from the company. Many times, companies offer free credit monitoring and explain how to enroll.
- Change your password(s) immediately. To ensure that you replace the current password with a strong password, choose one that is at least 12 characters and uses a combination of upper- and lowercase letters, numbers and special characters.
- Create a unique password. Do not recycle passwords that you might use for other accounts. If the password used for the breached account is one you use on other accounts, remember to change the password on all applicable accounts.
- Use multifactor authentication, which requires an additional step after you log into your account – such as a text to your cellphone – to gain access to that account. Multifactor authentication provides an extra layer of security.
- Review any bank account or payment method tied to the data breach. This might include credit cards, peer-to-peer payment platforms and bank cards.
- Check your credit report. You can check your credit report weekly at www.annualcreditreport.com through the end of 2023. You may want to put a fraud alert on your credit reports by contacting any of the three major credit-reporting agencies (Experian, Equifax or TransUnion). You can also freeze all three of your credit reports by contacting each of the agencies. Putting a fraud alert or credit freeze on your reports won't affect your credit score, and the alert is free.

Consumers who suspect an unfair business practice or want help addressing a consumer problem should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

Beware of "dark patterns" on the internet

Have you ever bought something you thought was a one-time purchase, only to later notice recurring charges totaling much more than what you initially paid?

The Consumer Protection Section of the Ohio Attorney General's Office cautions Ohioans about digital "dark patterns," tactics that some companies use to sign you up for a subscription product or service you never intended to buy. Worse, sometimes these unintended purchases can be difficult to cancel.

Digital dark patterns manipulate online users into taking action they didn't intend to take. According to an article from Wired magazine, dark patterns also are used to make it difficult to unsubscribe to a company's services or emails.

"When you want to unsubscribe from a mailing list but the 'Unsubscribe' button is tiny, low-contrast and buried in paragraphs of text at the bottom of an email," the article says, "it's a strong sign the company is putting up subtle roadblocks between you and cancellation."

In June 2023, the Federal Trade Commission sued Amazon for allegedly using dark patterns to unlawfully sign consumers up for Prime subscriptions without their consent, charging those customers and then making it difficult to unenroll.

The suit maintains that the online shopping superstore's dark patterns made cancellation difficult by requiring consumers to hunt for the right place to cancel online and then click through complicated extra pages.

"Often," the suit says, "consumers would call Amazon's customer service, only to be referred back to the website to cancel, making the process even more frustrating."

To steer clear of unwanted charges while shopping online, the FTC and the Ohio Attorney General's Office recommend that you:

- **Monitor what goes into your online shopping cart.** Be sure to look closely for any wording or fine print that might enroll you into a subscription service. Before finalizing an online transaction, be sure to review your entire order. Look for anything that has been added that you don't want, and remove it from the order.
- **Look for boxes that might be pre-checked to enroll you in a subscription service unless you uncheck the box.**
- **Double-check the order confirmation you receive by email from the company.** If there is an item or subscription service that you didn't intend to sign up for, immediately contact the company to cancel and secure a refund. Request that you receive written confirmation of your

cancellation, and save it in case you need documentation later. If the company says you can keep the subscription, ask to cancel it and/or ask when the subscription is up for renewal so you can be sure it's canceled ahead of that date.

- **Carefully review your bank statements and credit-card-billing statements to ensure that you're not being charged for subscriptions you don't want.** If necessary, dispute any unwanted charges with your credit- or debit-card company – especially if you've tried to cancel and the company has not honored the cancellation.

- **Look for any fine print about "auto renewals."** If you unwittingly enroll in an automatic renewal, typically you will continue to see charges unless or until you cancel. Sometimes auto renewals can be far off, such as one that bills a year after the "purchase."

Ohioans who suspect unfair or deceptive business practices should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

Holiday shopping: Research prices early, and save when you're ready to buy

Retail stores' holiday decorations – and store sales – seem to pop up earlier every year. Before the holiday season begins in earnest, why not do price comparisons now for items you want to buy – so you can save when you're ready to buy them?

Ohio Attorney General Dave Yost offers the following seasonal shopping tips:

- **Plan before you shop**. Carefully review ads and compare deals. Keep an eye out for important exclusions and limitations that must be disclosed in ads, even online. Check the details to see whether limited quantities of an item are available for sale, the sale price is valid during certain hours only, or other terms and conditions apply.
- **Research online reviews**. Be cautious about reviews posted with generic names and profiles without photos; they might be impersonating legitimate shoppers. Cross-reference customer reviews of the same products on different websites. Consistent reviews on several online stores can add validity to the feedback.
- **Check return policies**. In Ohio, sellers can set their own return policies, including policies of "no returns." But if a policy limits your ability to obtain a refund, a seller must clearly notify you of that policy before you complete the purchase. Also, be sure to check return policies, as they might change during the holidays.
- **Be aware of third-party sellers**. Many companies allow multiple vendors to sell products on their website. When purchasing an item from a company website, verify whether you're buying the item from that company or a third-party seller. The company's refund polices and warranties might differ from those of a third-party seller.
- **Watch for "free" offers**: Before signing up for a free trial of a product or service, scrutinize the details, especially if you're asked to provide a credit-card number or pay for shipping and handling. In many cases, signing up for the offer automatically enrolls you in a program that includes recurring charges.

- **Compare gift cards**. Not all gift cards are alike, so review the terms and conditions before you buy. In general, most gift cards must last at least five years, but fees might vary depending on the type of card, such as a single-store card or a prepaid network-branded card that can be used almost anywhere. Also, promotional cards such as those included free with a purchase might not have the same protections.
- **Keep all receipts**. Having a complete record of a sale can help you handle problems that arise after the purchase. Keep copies of receipts, sales agreements, advertisements, photos of products and other documentation until the transaction and billing process are complete.
- **Check delivery dates and fees**. Carefully review the expected delivery date and shipping costs before making a purchase. Find out whether you'll be charged return-shipping or restocking fees if you return the product. Also, pick up delivered packages promptly to prevent theft or damage outside your door.
- **Beware of package tracking scams.** A package tracking scam might involve an email alert, which informs you of a "delay" in the shipping of a package. The email either asks you to provide personal information or click on a link for additional information. Providing personal information, however, could lead to financial harm or infect your computer with malware. In addition to keeping your shipping confirmation email, keep track of the retailers you've ordered from. And don't click on links if you're unsure whether the sender is legitimate.
- **Monitor your accounts**. Regularly check your credit-card and bank accounts for unauthorized charges or unexpected activity. If you find problems, immediately notify your credit-card provider or bank. The sooner you identify a problem, the sooner you can work to correct it.

Consumers who suspect an unfair business practice or want help addressing a consumer problem should contact the Ohio Attorney General's Office at www.OhioProtects.org or 800-282-0515.

'Consumer Protection Up Close'

Consumer Protection Up-Close examines and explains cases filed by the Ohio Attorney General's Consumer Protection Section.

In collaboration with the Federal Trade Commission and law enforcement partners nationwide, Attorney General Dave Yost joined an initiative in July 2023 that expands the crackdown on illegal robocall operations responsible for inundating consumers with billions of unwanted calls.

Operation Stop Scam Calls builds on the ongoing efforts of Ohio and other states to combat the persistent problem of robocalls and other unlawful telemarketing.

"Our collective efforts – from this sweep to the Anti-Robocall Litigation Task Force and beyond – help us to expand our playbook, allowing us to outwit and defeat these perpetrators in their own arena," Yost said. "Our secret weapon is consumers – whom we urge to continue reporting illicit robocalls, so we can sever these unwanted illegal robocallers' connection once and for all."

The comprehensive initiative targets telemarketers and lead generators who deceptively collect and provide consumers' phone numbers to robocallers, falsely representing that these individuals have consented to receive such calls.

Since taking office in January 2019, Yost has been working tirelessly to disconnect robocallers by targeting every link in the robocall chain. In the past two years, he has pursued numerous legal actions and consistently worked to educate the public.

Here's a timeline of the most recent work of Yost and his Consumer Protection Section:

- **July 7, 2022:** Yost files a lawsuit against 22 defendants – including California residents, Aaron Michael Jones, Roy M. Cox, Jr. and Stacey E. Yim – for their involvement in a massive "car warranty" robocall scheme. This ongoing case generated more than 1,600 complaints to Yost's office about unwanted calls. The defendants generated sales leads by using an unlawful and complex scheme to bombard consumers with more than 77 million robocalls a day.

- **Jan. 5, 2023:** Yost files a lawsuit against six individuals (including California resident Stacey E. Yim) and six companies that relied on illegal robocalls to generate sales leads, subsequently pitching "car warranties" to Ohio residents. The complaint alleges that Florida-based Pelican Investment Holdings financed leads to initiate outbound prerecorded calls, marketing and selling "vehicle service contracts."

- **March 7, 2023:** Yost reaches settlements with John C. Spiller II and Jakob A. Mears, operators of Texas-based Rising Eagle Capital Group, JSquared Telecom, and Rising Eagle Capital Group-Cayman. The two were responsible for initiating more than 69 million robocalls to phone numbers associated with Ohio area codes.

- **May 23, 2023:** Co-leading the Anti-Robocall Multistate Litigation Task Force, Yost sues Arizona-based Avid Telecom; its owner, Michael Lansky; and its vice president, Stacy Reeves, for violating the Telephone Consumer Protection Act and the Telemarketing Sales Rule, both federal laws. The complaint alleges that Avid Telecom, Lansky and Reeves knowingly provided substantial assistance or support to sellers and telemarketers engaged in illegal robocalling, including defendants involved in Yost's "car warranty" action filed in July 2022.

- **August 3, 2023:** Yost recognizes the FCC for imposing a record-breaking $299,997,000 fine against a multiplayer robocall enterprise. This penalty stems directly from the coordinated enforcement action taken in collaboration with the Ohio Attorney General's Office in July 2022.

- **August 17, 2023:** Yost announces judgments with the final defendants in the massive "health care" robocall operation. Under these judgments Scott Shapiro, Michael Theron Smith Jr. and Health Advisors of America – all of Florida – are subject to permanent robocall bans on calls to Ohio. In addition, Shapiro and Smith are barred for 10 years in Ohio from telemarketing, engaging in lead generation, providing or selling telephone numbers, and calling numbers listed on the Do Not Call registry. Shapiro is also banned for two years from participating in these activities nationwide.

Consumers who receive unwanted calls can complete an Unwanted Call Notification Form at www.OhioProtects.org. That information is directed to the Robocall Enforcement Unit, which uses the reports to identify trends to protect Ohioans.

SPOTLIGHT SERIES

Spotlight on … the Education Unit

The Education Unit of the Attorney General's Consumer Protection Section equips Ohioans with knowledge about their consumer rights and educates them about potential scams. The unit conducts consumer protection presentations throughout the state to build collaboration and awareness in the fight against fraud and to help protect Ohioans. In 2022, the Education Unit conducted 160 educational events, reaching 9,143 attendees.

The office has developed a number of consumer protection presentations to educate Ohioans about scams and consumer rights. Available topics include:

- Consumer Scams
- Cybersecurity Help, Information and Protection Program (CHIPP**)**
- Know Your Rights: A Consumer Guide for Students
- Protect Yourself from Identity Theft
- Senior Scams
- Shop Smart: Know Your Rights

These presentations are available both in person and in virtual formats, ensuring accessibility for groups of varying sizes. In-person presentations are generally scheduled on weekdays during business hours (9 a.m.–5 p.m.), with a 20-person minimum. Virtual presentations are available for groups of any size.

If your company, organization or club would like to host a consumer protection presentation, complete the online request form or contact us at 800-282-0515. Together, we can empower Ohioans to make informed choices and protect themselves from consumer-related scams and pitfalls.